Y/DW-1778

A Secure Sensor System for Protected Asset Remote Verification

J. R. Younkin, D. W. Carver, R. L. Lawson,
L. R. Mooney, C.A. Pickett, L.E. Seiber,

Y-12 Development Organization

July 8, 1999

To be presented at:
The INMM 40th Annual Meeting
The Pointe Hilton Resort at Squaw Peak
Phoenix, Arizona
July 25-29, 1999

Prepared by
Oak Ridge Y-12 Plant
Managed by
LOCKHEED MARTIN ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84-OR21400

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government of any agency thereof.

A Secure Sensor System for Protected Asset Remote Verification

J. R. Younkin, D. W. Carver, R. L. Lawson, L. R. Mooney, C. A. Pickett
L. E. Seiber

Lockheed Martin Energy Systems, Inc. *, P. O. Box 2009, Building 9203, MS-8084, Oak Ridge,
Tennessee 37831-8084

Abstract

The technology to securely perform data monitoring in remote locations has improved immensely in the past few years. A system using sensors with embedded microprocessors is being implemented to ensure the integrity, authenticity, and confidentiality of measured physical attributes of protected assets during remote verification. The transactions in a verification system must guarantee that the information has been generated by trusted sources, has not been altered, and is protected from disclosure to unauthorized personnel.

The Secure Sensor System architecture utilizes a hierarchical approach allowing each tier's security requirement to be individually addressed. At the local storage facility, the system consists of microprocessor-embedded sensors, sensor controllers, and facility database clients. Sensor readings and alerts in the facility database can be viewed locally with the Graphical Facility Information Center (GraFIC^{TM}) system. GraFIC^{TM} is also used at the remote verification site to observe those same sensor readings and alerts. Information transactions between the tiers as well as between the storage site and verification site occur with encryption and certification technology.

The smart sensors use low power components and techniques, communicate to a sensor controller using a set of standard commands and responses, and have the capability to perform secure algorithms for data authentication.

INTRODUCTION

The sensor sub-system for the third generation of Continuous Automated Vault Inventory System (CAVIS III) is being developed for its deployment at the Y-12 Plant. The sensor sub-system provides the data and events associated with attributes of the assets being protected to the Graphical Facility Information Center (GraFIC™). GraFIC™ is an information system that provides an inexpensive and flexible method of remotely verifying complete "up-to-the-minute" inventory of those assets.

The sensor sub-system consists of weight and radiation sensors, a sensor concentrator, and an acquisition computer. A specification that defines sensor classes by their capabilities and how those sensors behave and interface with the sensor concentrator has been formulated. Newly designed sensors have embedded microcontrollers to allow a certain degree of data authentication and encryption to occur prior to data transmission. Having embedded microcontrollers integrated with the sensor also allows the sensor to perform self-diagnostics and generate event-driven alarms.

BACKGROUND Since the end of the Cold War, one of the Oak Ridge Y-12 Plant's major missions has been the storage of SNM. Department of Energy (DOE) orders require that the status of the SNM inventories be confirmed periodically. This inventory confirmation provides assurance that the SNM is secure and has not changed. Confirmation of inventory status involves the measurement of physical characteristics of the stored material, in this case weight and radiation level. These measurements, which are currently done manually, are very expensive, both in terms of time and in number of people required. In addition, there are security and safety concerns when the stored items are measured manually.

The Continuous Automated Vault Inventory System (CAVIS) was developed to provide a way of remotely performing the inventory confirmation. CAVIS is a hardware and software sensor system that is capable of obtaining weight and gamma ray signature measurements from stored SNM. However, the CAVIS system by itself provides no user interface and is limited to very short-term storage of sensor readings. The GraFIC™ system was conceived to provide those elements missing from CAVIS - an easy-to-use user interface and long-term storage of sensor readings and other data. In addition, GraFIC™ has been designed to provide intelligent facility management features for the storage areas. Early in the development cycle, the GraFIC™ team recognized that the features of GraFIC™ could have broader application, and so the system was designed to permit easy adaptation to other facility environments.

The initial implementation of GraFIC™ at the Oak Ridge Y-12 Plant utilizes the CAVIS sensor system to monitor SNM that is stored in Modular Storage Vaults (MSVs). An MSV (see Figure 1) is a concrete slab that contains twenty cells, each of which holds a canister of SNM. Each cell has a weight sensor and a radiation sensor.

An embedded controller (Sensor Concentrator) is attached to the side of the vault and monitors the sensors. These vaults are placed in stacks, ranging from one to five vaults in height, and a concrete lid is placed on top of each stack.

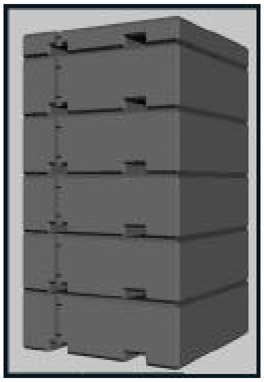

Figure 1 MSV Stack

A host computer commands the concentrators to scan all sensors at periodic intervals. The readings from these scans are saved in medium-term storage (for a few days) and sent to a database server for long-term storage. In addition, the host computer continually monitors the sensors via the concentrators and reports out-of-limits readings to the database server for instant alarm notification. The sensor concentrator accepts commands from the database server to do such things as alter its scan rate, download alarm limits, etc. GraFIC™ currently displays weight and radiation data from the stored SNM contained in those MSVs. An acquisition group host obtains this sensor data for GraFIC™ from sensor concentrators attached to the MSVs and having their associated sensors located in each storage cell. The latest deployment of CAVIS included sensor concentrators that had been retrofitted with a LonTalk® interface to facilitate installation as well as to provide data authentication. The operation of the sensor concentrator was also modified to allow sensor data values transitioning across threshold boundaries to generate messages indicating the state of the data values. This event-driven alarm notification mechanism was embedded in the sensor concentrator hardware to allow immediate notification of requested changes in sensor readings. The values for a sensor's low warning threshold, high warning threshold, low alarm threshold and high alarm threshold are calculated by GraFIC™ based on historical data and transmitted to the sensor concentrator.

Several CAVIS iterations have been implemented and successfully deployed in a SNM storage facility. The first CAVIS implementation (CAVIS I) was a 12 month layer test in this facility. The test allowed the CAVIS team to evaluate competing sensor technologies. Two types of weight and radiation sensors were evaluated during this phase. This included a fiber-optic weight pad and the capacitance weight pad. Tests were performed on the RadSIP, and two varieties of RadTELL. With the completion of the layer test, the best sensors were selected, and CAVIS II began. The CAVIS II phase was the first large-scale deployment into the SNM storage facility. This deployment included the GraFIC™ user interface. CAVIS III is a continuation of this effort offering improvements and additional features and capabilities to the original concept. The objectives of this concept are to develop a sensor system methodology for a multitude of assets, facilitate the installation of sensors, provide low cost and low power sensors, and to provide security mechanisms.

ACQUISITION NODE

The CAVIS acquisition node consists of the sensors and the sensor concentrator as depicted in Figure 2.

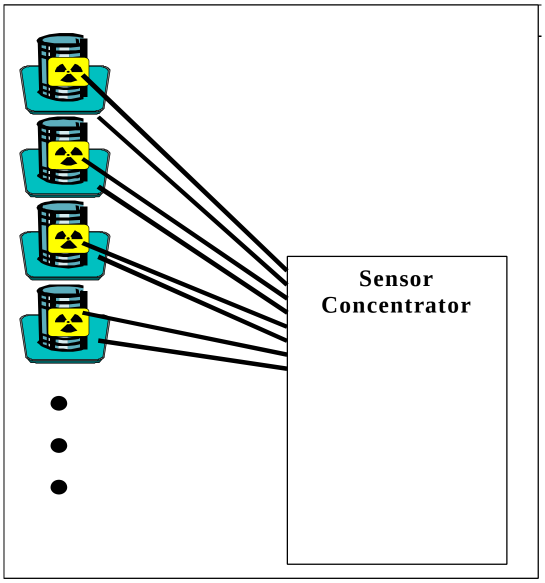

Figure 2 Acquisition Node

Communications between the sensor concentrator and the sensors are governed by the protocol defined in the system specification document. This document was written to define system features and capabilities. It details sensor concentrator capabilities, defines the mandatory requirements for full sensor concentrator support, details sensor classes and capabilities, and defines communications protocol.

The acquisition node incorporates LonWorks® Technology and event-driven alarm notification. Event-driven alarm notification was implemented in the sensor concentrator to provide timely notification of abnormal variations in sensor readings. The sensor concentrator transmits messages when sensor readings exceed established thresholds. A host computer will now not only periodically collect sensor readings but will also capture alarm notifications from the sensor concentrators.

<u>SENSORS</u> A key component in the sensor system is smart sensors. A section of the system specification document defines several different classes of smart sensors and their mandatory/optional features. Though the sensors are expected to contain some computing power, an unsophisticated smart sensor can be designed around most micro-controllers.

Currently three types of sensors are under development. A conceptual design to upgrade the CAVIS II capacitance weight pad exists. This design is based on the ATMEL AT90S2313. A similar upgrade to the RadSIP sensor has been designed and is also based on the AT90S2313. A prototype smart sensor for weight and radiation has been designed. This sensor is designed around the Analog Devices ADUC812 Microconverter.

SMARTPAD SmartPad is a sensor designed to meet the goals defined for the Y12 deployment. One requirement of CAVIS is that at least two physical attributes of an SNM be measured. To meet this requirement SmartPad integrates weight and radiation measurements in a single package. To minimize the impact of hardware failures, SmartPad is designed such that each measurement is performed by independent hardware. Dedicated processors are utilized to implement each measurement with smart sensor protocols. SmartPad is designed for use in large sensor networks and has built-in features to facilitate network installation. Theoretically, SmartPad can operate with power consumption less than 100 milliwatts. From a manufacturability standpoint, the SmartPad's simplistic mechanical design lowers production costs. This mechanical design is adaptable to various container sizes. Implemented with low cost sensor technology, SmartPad is a cost effective and manufacturable solution for weight and radiation measurement.

SENSOR CONCENTRATOR The sensor concentrator is an intelligent data acquisition unit incorporating LonWorks® Technology for allowing the data of 40 sensors to be easily and reliably accessed on a low cost twisted pair network. Ideally suited for monitoring applications, the sensor concentrator acquires and filters sensor data and can immediately alert network devices when signal levels cross four user-defined thresholds. The sensor concentrator also provides power for the sensors.

The unit contains 22 microcontrollers. There is a master controller, an Echelon network controller, and one communications controller for each pair of RS-485 sensor channels. A Motorola 68HC11 microprocessor manages the communications microcontrollers and the communications protocol with the sensors as well as the handling data authentication and encryption. The 68HC11 microprocessor has 32K of local non-volatile storage. The 68HC11 microcontroller interfaces with an Echelon 3120 Neuron® processor running at 5 MHz to reduce power consumption via a synchronous serial interface. The neuron processor uses its embedded LonTalk® communications protocol to connect to a twisted-pair wiring 78.1Kbps free topology network. The LonTalk® protocol is an open communications protocol and a de facto standard for industrial control applications [1]. LonTalk® also provides reliable communication services [1]. The sensor concentrator connects to a Free Topology network. Once connected, the sensor concentrator communicates with other networked devices and host computers via network variables.

The LonTalk® protocol session layer service of the Neuron processor in the sensor concentrator provides authentication of the generated sensor data by verifying the identity of sensor concentrator providing the data. This authentication mechanism uses a challenge/response scheme that requires a response to a challenge during each data transmission.

SENSOR COMMUNICATIONS PROTOCOL The system specification document (SSD) defines the protocol used by sensor concentrator in communicating with sensors. The protocol is defined to allow data acquisition, encryption, and authentication, sensor configuration and diagnostics as well as network management features all via a common sensor interface. Auto-detection of new sensors is supported to facilitate sensor installation. The SSD defines methods to launch local diagnostic routines and diagnostic routines for attached sensors.

DATA AUTHENTICATION Data Authentication ensures the source of the data has not been compromised. A unique ID is assigned to each smart sensor and sensor concentrator. At the time of installation, each sensor is added as an authorized data source, and sets its host as an authorized command source. For data and command transactions, the sender/receiver identification is checked. A transaction received from an unauthorized source is an illegal transaction. The acquisition node host is notified of illegal transactions. An illegal transaction log is automatically generated at the sensor concentrator.

DATA ENCRYPTION The secure sensor system utilizes data encryption to maintain confidentiality of the data generated by installed sensors. The system specification defines an encryption implementation, which focuses on securing transmissions between sensors and their sensor concentrator. Although the default encryption scheme is a dynamic key-based algorithm, other encryption schemes can be implemented.

ACQUISITION GROUP

An acquisition group is a sensor sub-system consisting of multiple acquisition nodes and an acquisition host computer.

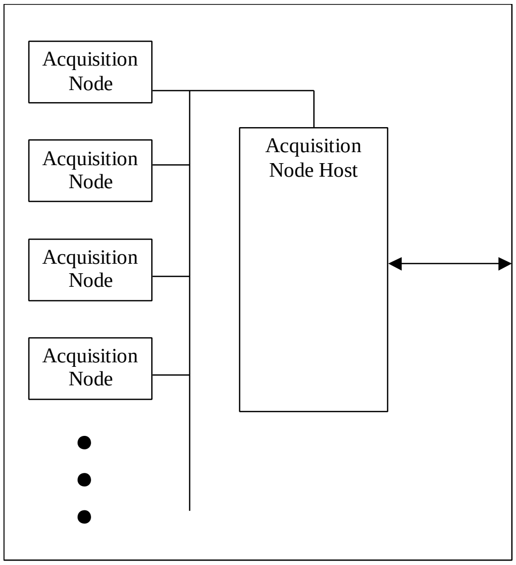

Figure 3 Acquisition Group

The Acquisition node host interfaces to the GraFIC information system. It acquires data from acquisition nodes via periodic scans and event notifications, provides several days of medium-term data storage, and sends data to the GraFIC database for long-term storage. The acquisition node host consists of a data collection service to read the sensor data at a user selectable period, a change-of-state service to capture the alarm notifications of the sensors and a configuration service to configure the thresholds on which the sensor alarm notifications are triggered. The acquisition host implementation is based on the Echelon® Corporation LonManager® Dynamic Data Exchange (DDE) Server. Inter-application communication via dynamic data exchange is used to monitor and update LONWORKS® network variables [2]. The acquisition host components change-of-state service, configuration service, and data collection service participate in DDE conversations with the LonManager® DDE server to receive information from and send information to the acquisition nodes. An Echelon® PCLTA interface card is used in the acquisition host computer to allow it to act as a networked device on the LONWORKS® control networks.

ACQUISITION STATION

An acquisition station consists of one or more acquisition groups, a GraFIC™ database server, one or more GraFIC™ client workstations and an Internet Protocol line encryption/decryption device [3]. Although the GraFIC™ system adheres to a client-server model, the server and all client software could be run on a single system, but a more typical arrangement is depicted in Figure 4. The acquisition groups provide the periodic sensor readings and report alarm conditions to the database server for instant alarm notification.

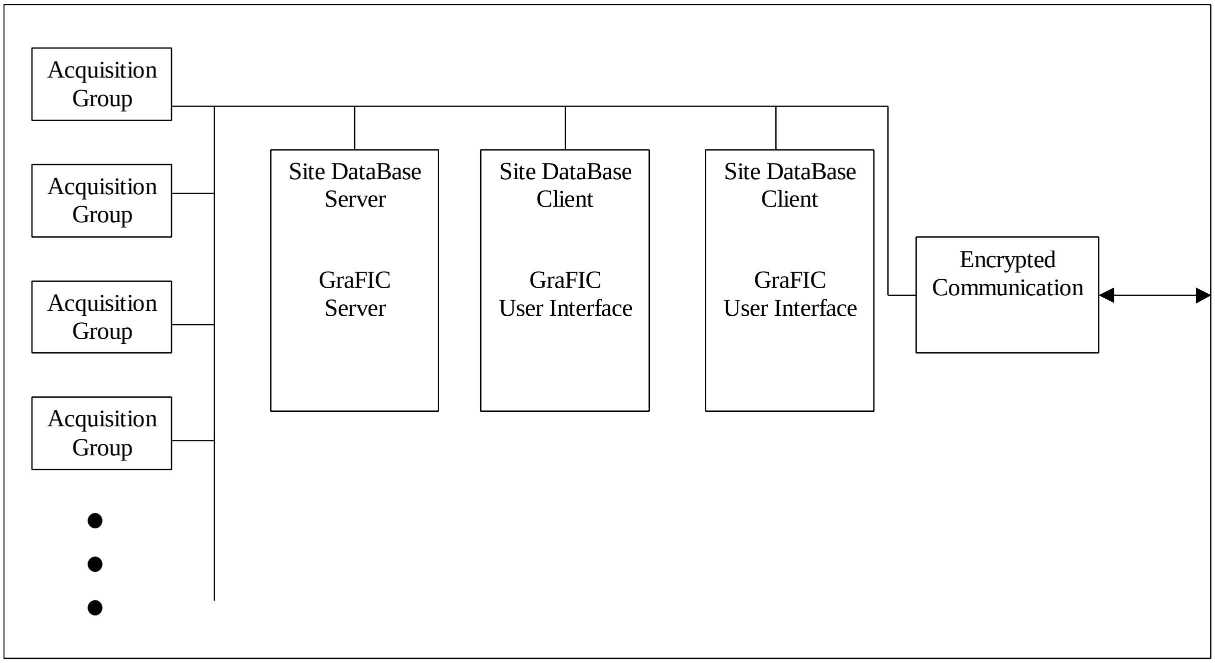

Figure 4 Acquisition Station

An acquisition station installation may have one or more workstations to provide access to the user interface. These workstations may be placed in locations that are convenient to the workers who need to use them.

REMOTE MONITORING STATION

A remote monitoring station installation may have one or more workstations to provide views into the acquisition stations as would be accomplished locally. Both current and historical information can be accessed. GraFIC™ maintains a history of events that has occurred allowing both local and remote operators to look back in time on previous events.

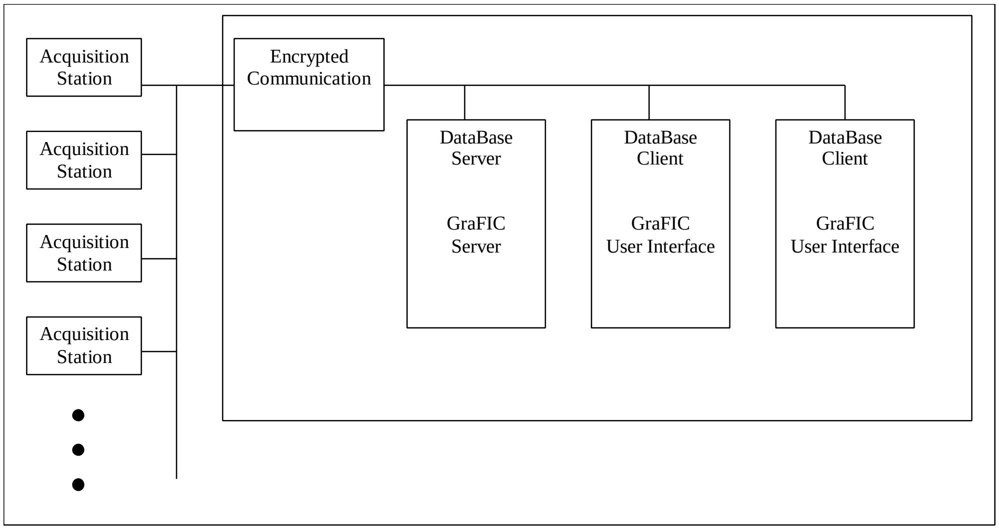

Figure 5 Remote Monitoring Station

SECURITY/ADMINISTRATION

Because GraFIC™ is designed to run on a Windows NT system (or systems), the well-known security features of Windows NT are available. The GraFIC™ application is built on a multi-tiered security model. GraFIC™ users fall into several categories, and the user interface features available depend on the user's category. Since the security model is implemented using Oracle™ roles, this protection is enforced even when other products, such as browsers or ad-hoc query tools, are used to access the database. The GraFIC™ application enforces a two-person rule for configuration updates and alarm acknowledgement. Under this rule, two privileged users must log onto GraFIC™ before updates or alarm acknowledgements can be made.

Both the remote Monitoring station and the Acquisition station can provide two encryption mechanisms to maintain the confidentiality of the data. Line encryption exists between these stations and the TCP/IP Network that they connect for protecting data as it moves between them. Local encryption of the stored data at either station type can also be performed to protect data from unauthorized access [3].

FUTURE WORK

Smart Card technology development will continue to provide improved information security mechanisms. Future CAVIS sensor development will attempt to incorporate similar technology.

The same cryptographic co-processors that are currently being used in smart cards to perform encryption, signatures, and verification can also be used with the embedded controllers contained in the sensors [4]. Designs of smart sensors with this type of hardware will be investigated for future implementation.

SUMMARY

The CAVIS hardware development cycle has continued to follow an evolutionary prototyping model. Several refinements and changes to CAVIS features and subsystems as well as the incorporation of new features have occurred, building on the successes of previous CAVIS deployments.

A significant effort has been made in the formulation of the Sensor Specification Document - a blueprint of a secure sensor system. Newly designed sensors having embedded microcontrollers based on this specification have been prototyped and are being tested. These sensors will allow a certain degree of data authentication and encryption to occur prior to data transmission, perform self-diagnostics, and generate event-driven alarms.

GraFIC™ provides a graphical user interface and long term data storage for sensor sub-systems. Equipped with GraFIC™, CAVIS III will provide fast and inexpensive SNM inventory status confirmation, real-time alarm notification and other storage facility management features for the Oak Ridge Y-12 Plant.

REFERENCES

[1] Echelon Corporation, Interoperable Control Networks Using LONWORKS® Technology, LONWORKS Workshop Presentation.

[2] Echelon Corporation, LonManager™: DDE Server User's Guide, Version 1.5 User's manual.

[3] J.G.M. Goncalves, W. Sequeira, F. Sorel, "Internet Based Multimedia Interfaces for Remote Monitoring and Surveillance," INMM/ESARDA Workshop on Science and Modern Technology for Safeguards, Sept. 21-24, 1998, Albuquerque, New Mexico.

[4] Henry Dreifus, J. Thomas Monk, Smart Cards, John Wiley and Sons, Inc., New York, 1997.

[*] Managed by Lockheed Martin Energy Systems, Inc. for the U. S. Department of Energy under contract DE-AC05-84OR21400.